Tutorial – Facial Recognition

Introduction:

Biometrics are best defined as the science of using unique physiological or behavioral characteristics to verify the identity of an individual. Biometric characteristics are unique to individuals and cannot be lost or stolen like passwords, making them not only convenient but also more effective in the prevention of theft or fraud. They include fingerprints, iris scanning, hand geometry, voice patterns, facial recognition and other techniques. Biometrics are of interest in any area where it is important to verify the true identity of an individual.

Biometrics are not a panacea for all our personal identification related issues, but an enhancing tool in our technology toolbox. A great amount of technical progress has been made, providing more accurate and more refined products. The unit cost is dropping to a level, which makes them suitable for broader scale application. The knowledge base concerning their use and integration into other processes has increased dramatically.

Currently, biometric technologies are employed in a broad range of public-facing situations. One of which is facial technology. This technology employs the use of a sensor, algorithm, and matcher technology to aid in the identification or verification of an individual. This tutorial will discuss this technology.

In recent years, there has been much interest in facial recognition techniques. Facial recognition offers the potential of a non-contact technology, although various groups are reviewing privacy act issues.

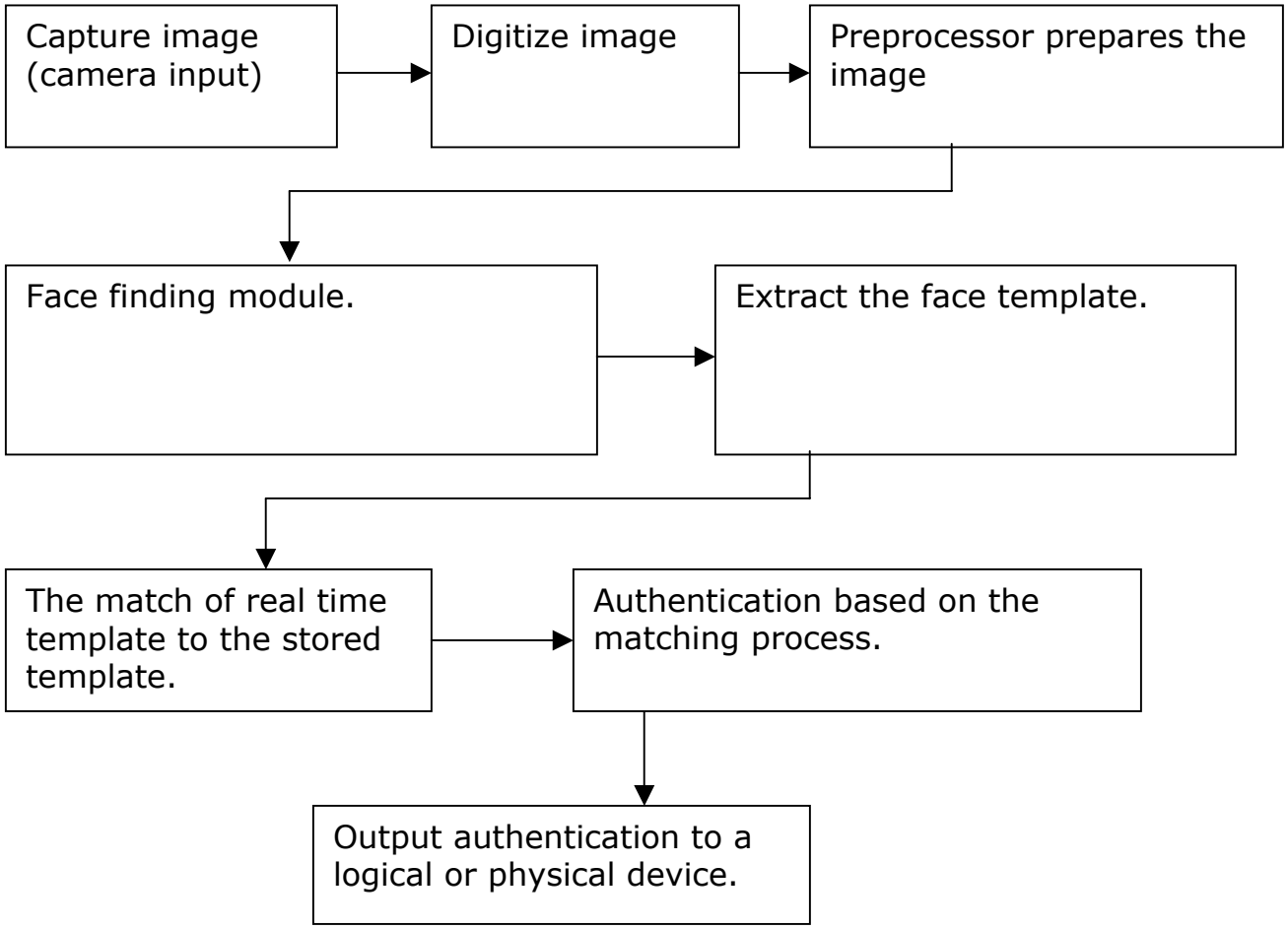
Types of Authentication Methods:

The two types of authentication are "Identification" and "Verification". These are sometimes confusing to people when discussing biometrics. The majority of biometric devices operate in the verification mode. The means that an identity is proven by calling a particular template from storage (invoked by the use of PIN, token or user-id) and then the person presents the live sample of their biometric for comparison, which results in a match or no match according to the predefined threshold parameters. This is known as a one-to-one (1:1) method of verification that may be performed quickly as the result of comparing the template to live sample/biometric.

The other match is a one-to-many (1:m), which is where the person submits their biometric for identification and the system attempts to identify the person from a database of templates. The user presents the biometric sample and the database engine starts the search. The system will search to find the correct identified person that matches the live sample. The one-to-many methodology operational speed is based on the biometrics used and the size of the database.

Using the one-to-one methodology will be faster than the one-to-many. The search is limited and the comparison is only against a limited number of templates.

Facial Recognition Overview:



The facial recognition technology has attracted considerable interest and whose capabilities are being more understood daily by the public. It is one thing to match two static images, it is quite another to unobtrusively detect and verify the identity of an individual within a group. It is easy to understand the attractiveness of facial recognition from the user perspective, but facial recognition technology progress continues to improve; it will be interesting to see how future implementations perform.

Facial Recognition Systems:

The facial recognition systems relies on a clean image to process. Using a variety of cameras can capture the image. Generally, the facial recognition system camera selection can be a video camera, closed circuit TV camera, surveillance cameras, digital camera, or an infrared camera. The key issue is that the camera produces a clean image that can be processed by the facial recognition technology. The application will determine what would be the correct camera for the solution. The camera can be a separate purchase or the use of the current camera system may be used if the quality provides the correct image.

There are various systems using a different approach to facial recognition. The following will show how some of the facial recognition systems use their algorithm to build the database.

The use of eigenface[1], which is the mathematical algorithm translating the characteristics of a facial geometry into a unique set of numbers. The eigenface is used for both identification and verification in real-time. The software can calculate an individual's eigenface from either a live video or a still digital image, and then search a database of millions in a few seconds in order to find similar or matching images.

Another vendor uses what is called the Local Feature Analysis[2], which is a mathematical technique developed by the vendor. The system takes the whole face and sub divides the face into different areas. The system then process the areas with mathematical algorithm and with the best results from each area places all the areas together for the final template. The system has enough redundancy and robustness to compensate for blinking, smiling, frowning, facial hair, eyeglasses, or hairstyle.

Still another vendor uses the three-D recognition system[3], which looks at the whole face, not at a fixed number of points. The system sees the entire face as you would. This uses a patented Holgraphic/Quantum Neural Technology, which is not based upon a commonly used algorithm but the quantum property of nature.

Facial Recognition Process:

How does all of this work? All biometric devices and systems have their own methodology, algorithms, and techniques. The matcher

algorithm is the heart of the facial recognition system. The algorithm is the key in tracking a person's face in facial recognition biometrics.

Initially a person will enroll, which needs to happen before we can verify the person's identity. The enrollment is to first "capture" a sample of the person on a biometric template. This captured template is the reference data that the future sample is compared to at the verification or identification stage. A number of samples are captured, during the enrollment phase, to get the best template that will be used in the process.

If a live person is not available to enroll a photograph or an artist rendered image can be used to capture the person's identity so that when the face is found, it will identity the person.

The template can be referenced with a Pin, Token or other means of identification in order to recall it for comparison with the live sample. If the database uses one-to-many matching, then no other items are linked to the template. The enrollment process and quality of the template are critical factors in the overall success of the biometric application. If a poor template is generated by the capture during the enrollment process, the subject will be required to re-enroll.

The templates can be stored in a variety of applications. The template can be stored on the biometric device, a central repository (server or web) or on a smart card. There are advantages and disadvantages to all of these methods. If the biometric is stored on the device, it will be faster and self-containing; however, the templates can become vulnerable to other forces such as if the device fails. Then there will be a need to reload the template database or re-enrolling the users.

If storing the templates in a central repository is the option, it will provide an additional level of security to the network. Each template can vary between 9 bytes and 1.5 kilobytes. If the network fails and access to the central repository is unavailable, access to a system or a door could be denied. There are methods to utilize in order to avoid an "access denied" by the authorized users.

If the biometric is stored on a smart card, the user has their biometric with them at all times. A downside to this could be once the user loses their card; they have lost their biometric. Each application needs to explore the requirements for the user and the security level of operations that are required in each organization.

The biometric template should be encrypted during storage and transmission of the template. This provides a level of security that truly enhances any physical or logical access program for an organization.

Areas of concern:

There are some areas of concern using facial recognition, as there would be when putting any system into an application.

There are some major causes of face recognition failure or diminished performance. If long hair is blocking or obscures the central part of the face this would create a problem in facial recognition. When the system is installed the lighting needs to be reviewed for the best performance for the system.

A high glare on eyeglasses could possibly cause a problem. There are solutions for this problem the main one is that it can be overcome by adjusting the lighting.

The angle in which the facial recognition system is attempting to track the subject loses the probability of the matching ability as the degree of angle increases from the front of the face to the side. This could create a problem in the area of surveillance.

Each application needs to be reviewed based on the facts and the use of biometrics. There may be concerns but with proper preparation and using the correct solutions the concerns may be overcome.

---

[1] Viisage Technology
[2] Visionics Corporation
[3] AcSys Face Recognition System